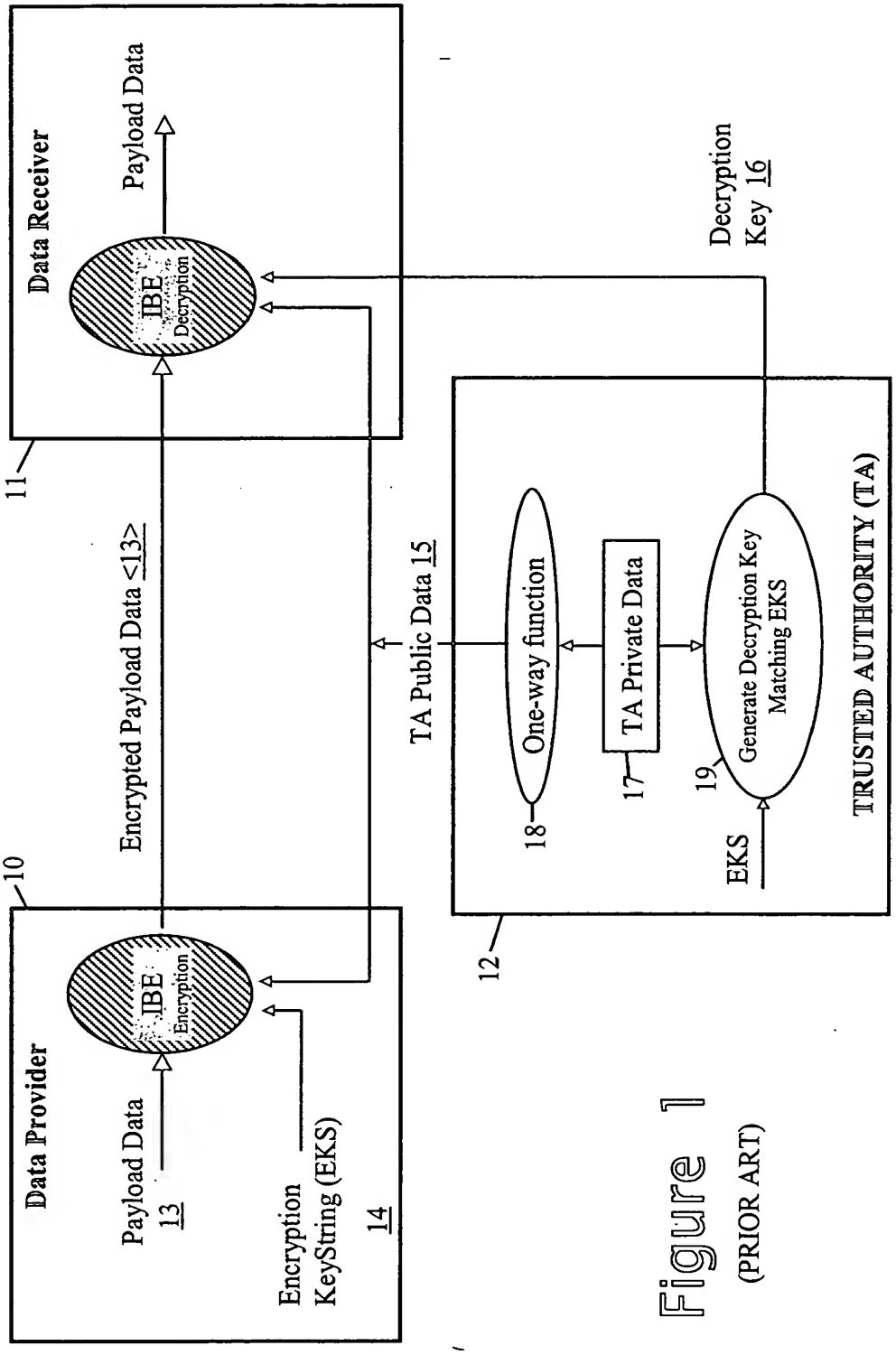
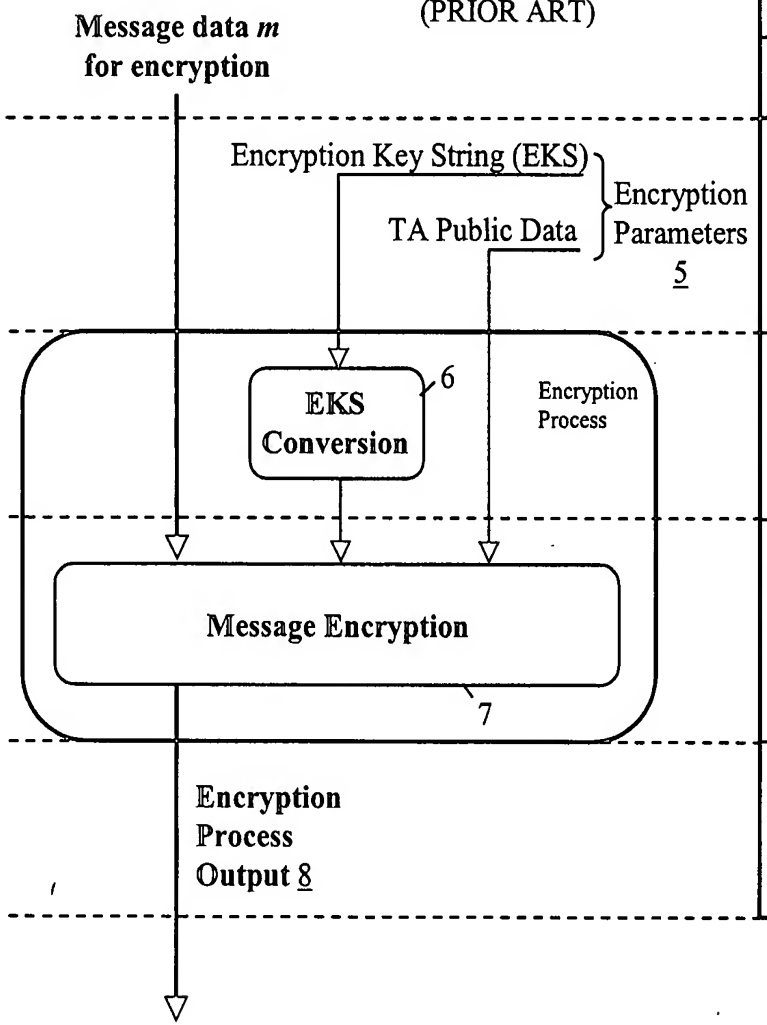


Figure 1
(PRIOR ART)

Figure 2

(PRIOR ART)



Identifier-Based Method		
Quadratic Residuosity	Bilinear Mappings $\hat{p}: G_1 \times G_1 \longrightarrow G_2$	RSA Based
EKS Modulus N	EKS (P, sP) where P is in G_1 s is secret of TA	EKS Modulus n
$K = \#(\text{EKS})$	"Map-to-point" hash $Q_{ID} = H_1(\text{EKS})$ *where* $H_1: \{0,1\}^* \longrightarrow G_1$	e = #(EKS)mod n
For each bit: $s_+ \equiv (t_+ + K/t_+) \bmod N$ $s_- \equiv (t_- - K/t_-) \bmod N$	$V = m \oplus H_2(t\,(sP, rQ_{ID}))$ *where:* $H_2: G_2 \longrightarrow \{0,1\}^*$ r is a random number	$m^e \bmod n$
For each bit: s_+ s_-	V, $U\,(= rP)$	$m^e \bmod n$

(knowledge of EKS and TA concerned also needs to be available)

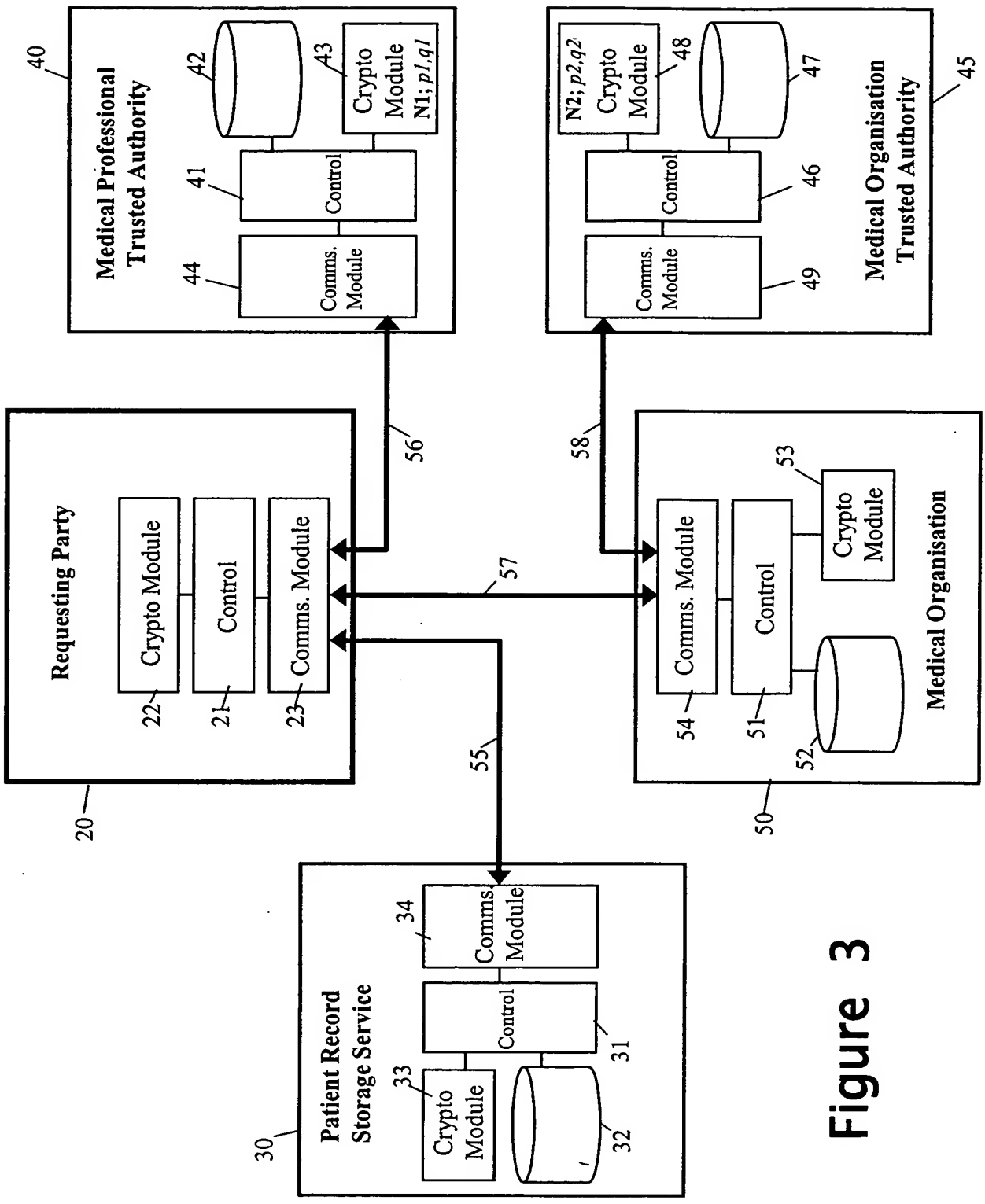

Medical Professional Trusted Authority
40
42
43
Crypto Module N1; p1,q1
41
Control
44
Comms. Module
Medical Organisation Trusted Authority
45
N2; p2,q2
Crypto Module
48
47
46
Control
Comms. Module
49
Requesting Party
20
Crypto Module
22
Control
21
Comms. Module
23
56
58
57
55
Medical Organisation
50
Comms. Module
54
Control
51
Crypto Module
53
52
Patient Record Storage Service
30
Crypto Module
33
34
Comms Module
Control
31
32

Figure 3

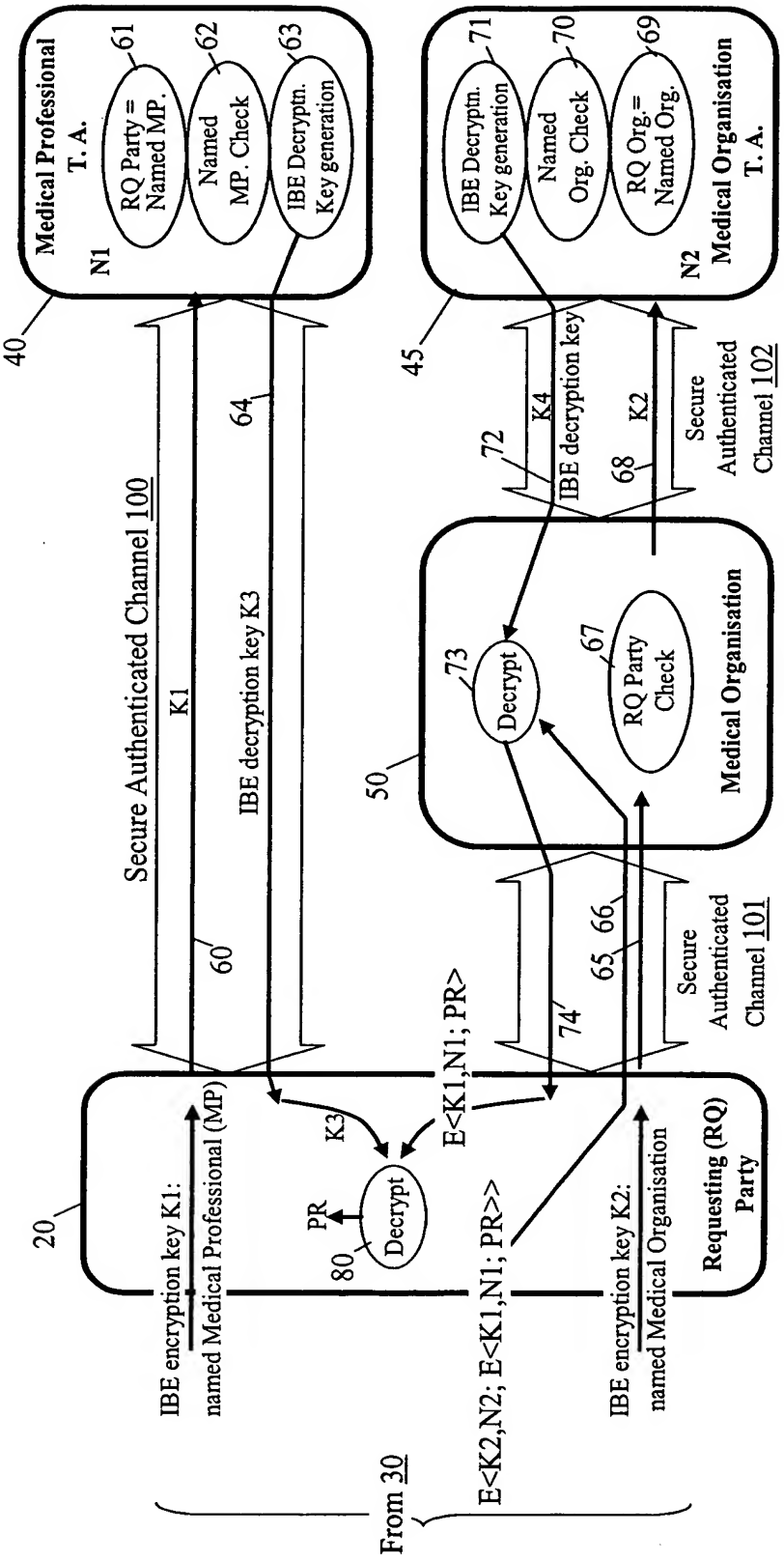

Medical Professional T. A.
N1
RQ Party = Named MP.
Named MP. Check
IBE Decryptn. Key generation
61
62
63
40
Secure Authenticated Channel 100
K1
IBE decryption key K3
64
60
IBE Decryptn. Key generation
Named Org. Check
RQ Org.= Named Org.
Medical Organisation T. A.
N2
71
70
69
45
IBE decryption key
K4
K2
72
68
Secure Authenticated Channel 102
50
Decrypt
RQ Party Check
73
67
Medical Organisation
Secure Authenticated Channel 101
66
65
74
E<K1,N1; PR>
20
IBE encryption key K1: named Medical Professional (MP)
K3
PR
80
Decrypt
E<K2,N2; E<K1,N1; PR>>
IBE encryption key K2: named Medical Organisation
Requesting (RQ) Party
From 30

Figure 4

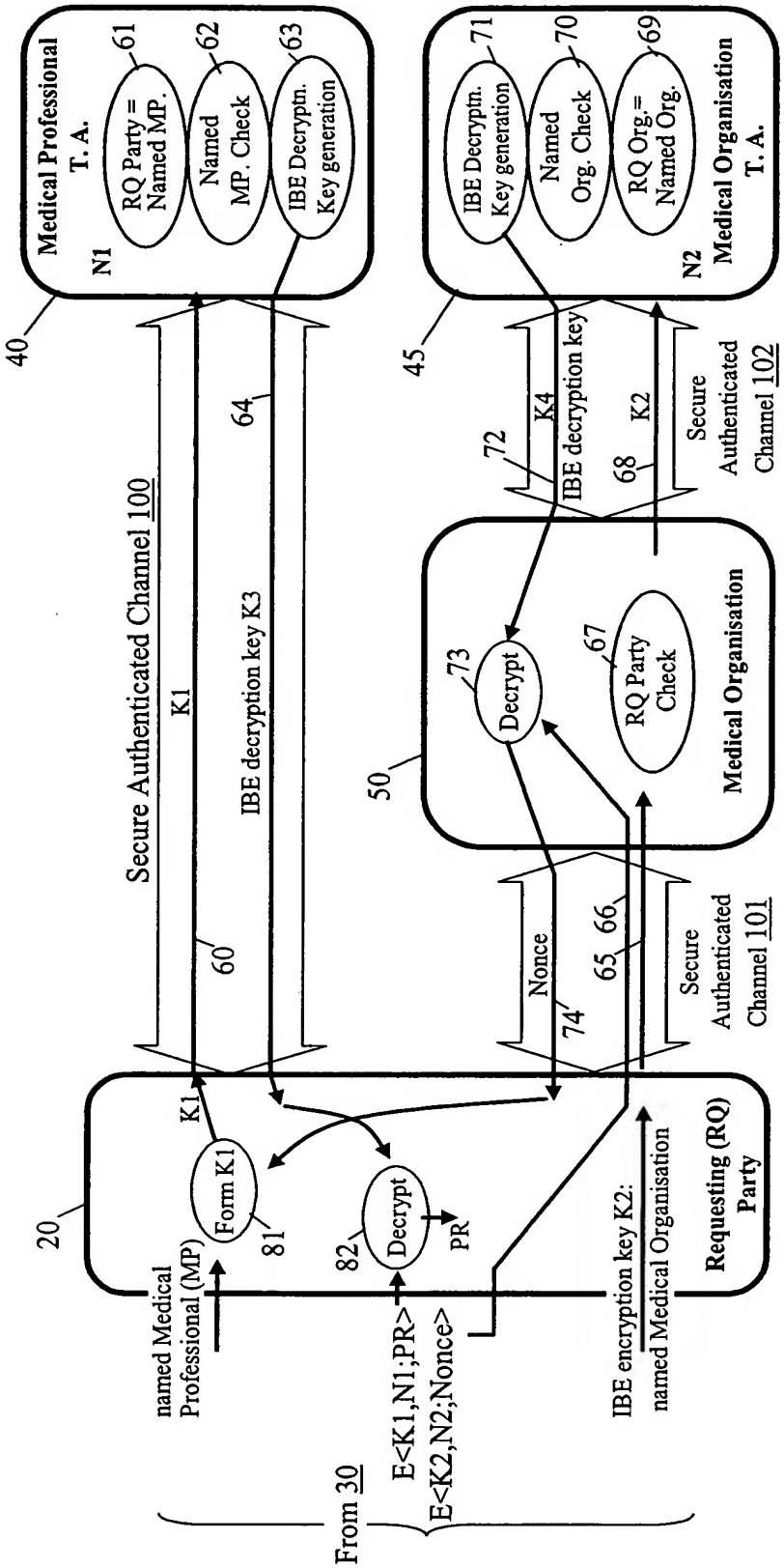

Medical Professional T. A.
N1
RQ Party = Named MP.
Named MP. Check
IBE Decryptn. Key generation
61
62
63
40
Secure Authenticated Channel 100
K1
IBE decryption key K3
64
60
IBE Decryptn. Key generation
Named Org. Check
RQ Org.= Named Org.
N2
Medical Organisation T. A.
71
70
69
45
72
K4
IBE decryption key
68
K2
Secure Authenticated Channel 102
50
Decrypt
73
RQ Party Check
67
Medical Organisation
Nonce
74
65
66
Secure Authenticated Channel 101
20
K1
Form K1
81
82
Decrypt
PR
Requesting (RQ) Party
named Medical Professional (MP)
E<K1,N1;PR>
E<K2,N2;Nonce>
IBE encryption key K2:
named Medical Organisation
From 30

Figure 5

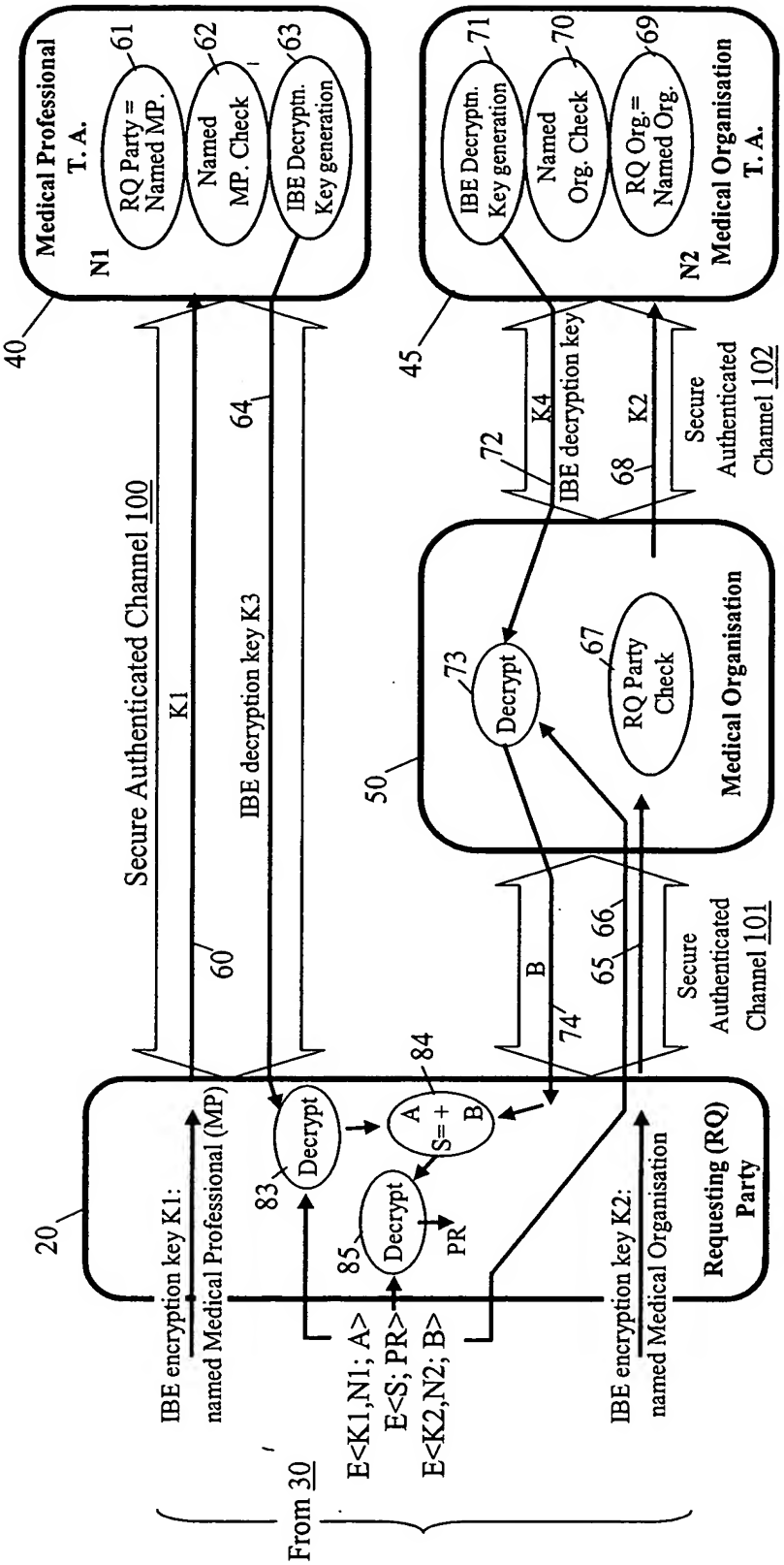

Medical Professional T. A.
N1
RQ Party = Named MP.
Named MP. Check
IBE Decryptn. Key generation
61
62
63
40
Secure Authenticated Channel 100
K1
IBE decryption key K3
64
60
45
IBE Decryptn. Key generation
Named Org. Check
RQ Org.= Named Org.
71
70
69
Medical Organisation T. A.
N2
72
K4
IBE decryption key
68
K2
Secure Authenticated Channel 102
50
Decrypt
73
RQ Party Check
67
Medical Organisation
B
74
65
66
Secure Authenticated Channel 101
20
IBE encryption key K1:
named Medical Professional (MP)
Decrypt
83
A
S= +
B
84
Decrypt
85
PR
E<K1,N1; A>
E<S; PR>
E<K2,N2; B>
IBE encryption key K2:
named Medical Organisation
Requesting (RQ) Party
From 30

Figure 6

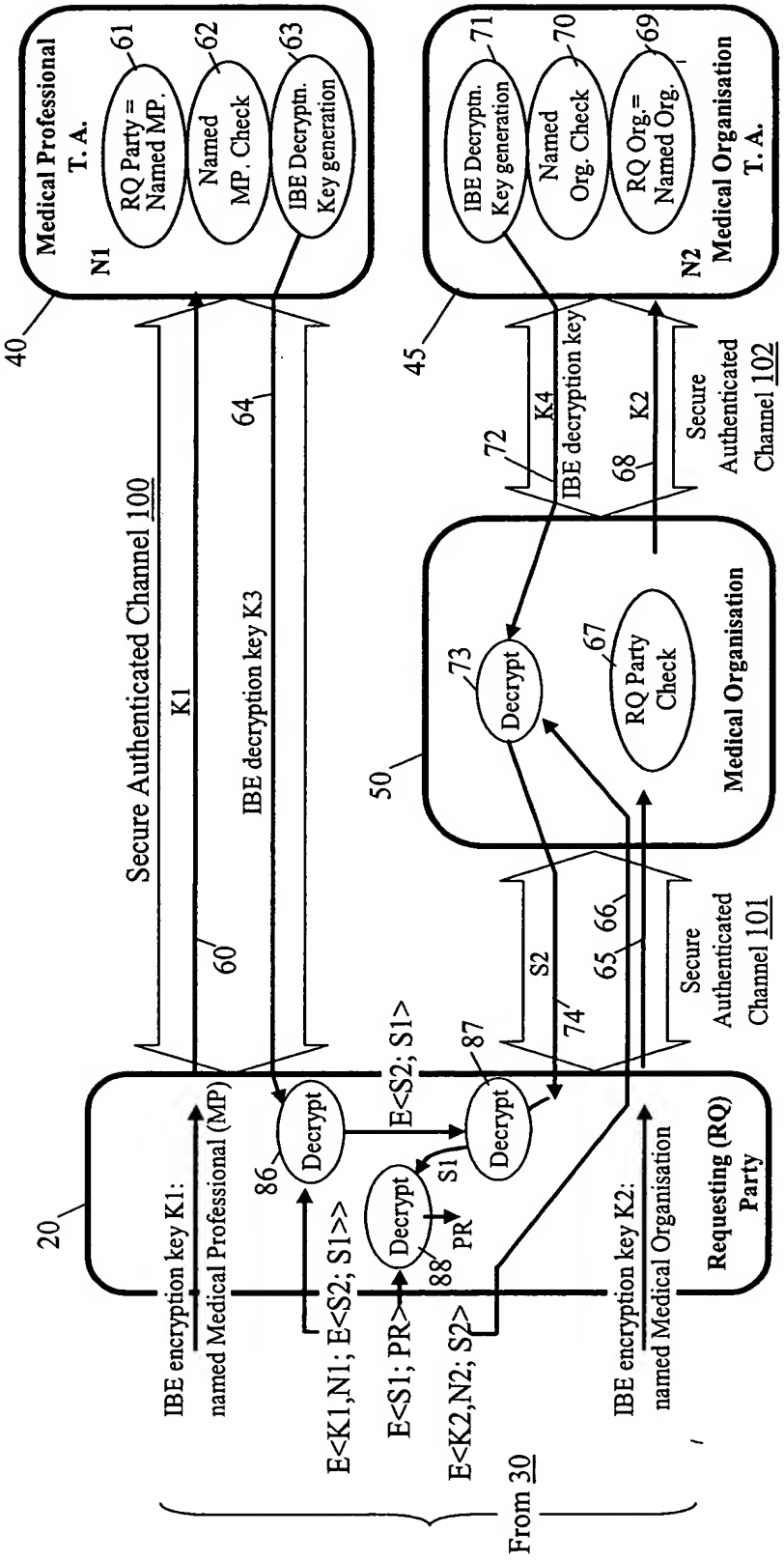

Medical Professional T. A.
N1
RQ Party = Named MP.
Named MP. Check
IBE Decryptn. Key generation
61
62
63
40
Secure Authenticated Channel 100
K1
IBE decryption key K3
64
60
45
IBE Decryptn. Key generation
Named Org. Check
RQ Org.= Named Org.
Medical Organisation T. A.
N2
71
70
69
72
K4
IBE decryption key
68
K2
Secure Authenticated Channel 102
50
Decrypt
73
RQ Party Check
67
Medical Organisation
S2
74
65
66
Secure Authenticated Channel 101
20
IBE encryption key K1: named Medical Professional (MP)
E<K1,N1; E<S2; S1>>
E<S1; PR>
E<K2,N2; S2>
86
Decrypt
E<S2; S1>
87
Decrypt
S1
Decrypt
PR
88
IBE encryption key K2: named Medical Organisation
Requesting (RQ) Party
From 30

Figure 7

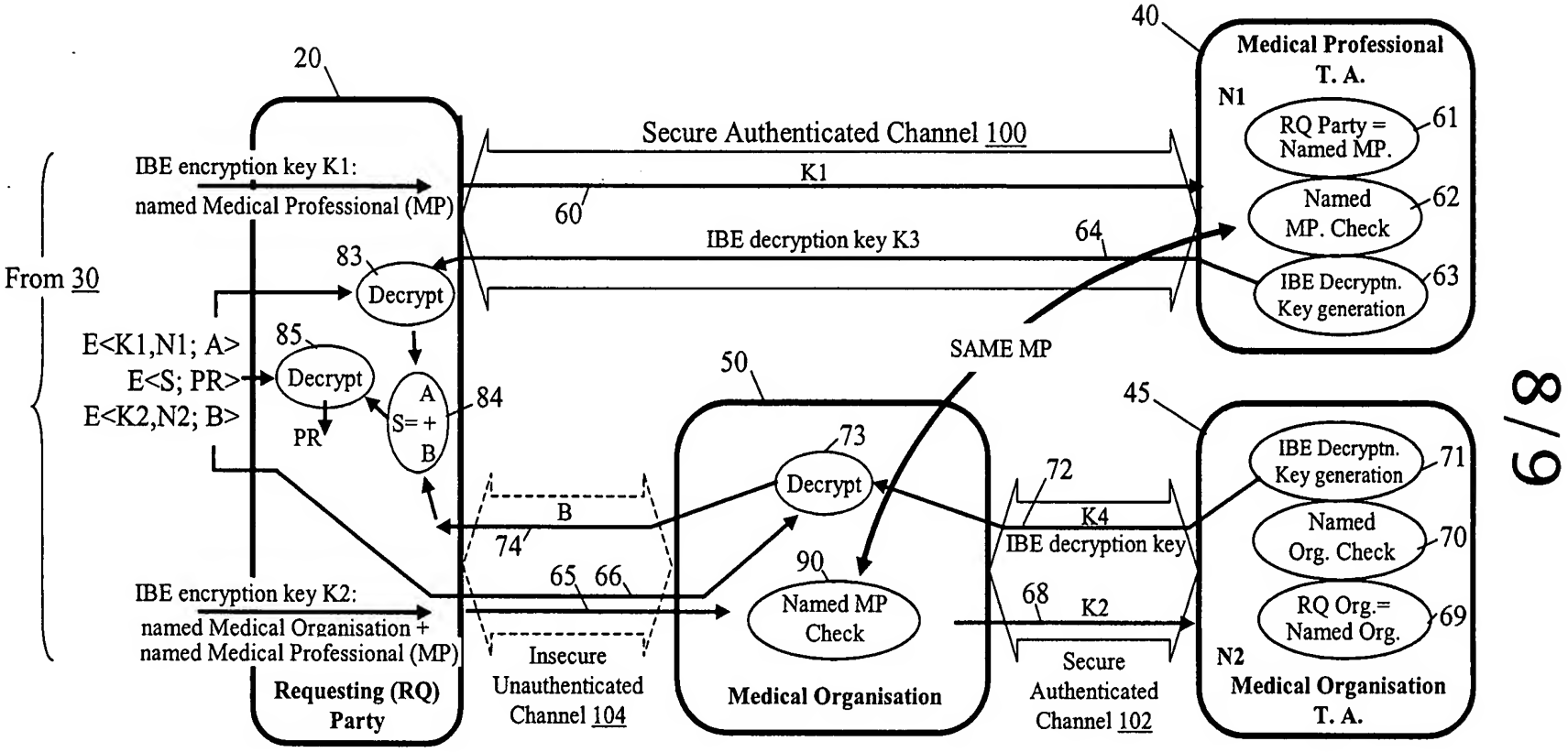

20
40
Medical Professional
T. A.
N1
RQ Party =
Named MP.
61
Named
MP. Check
62
IBE Decryptn.
Key generation
63
Secure Authenticated Channel 100
K1
60
IBE encryption key K1:
named Medical Professional (MP)
IBE decryption key K3
64
From 30
83
Decrypt
E<K1,N1; A>
E<S; PR>
E<K2,N2; B>
85
Decrypt
PR
A
S= +
B
84
SAME MP
50
45
73
Decrypt
72
K4
IBE decryption key
IBE Decryptn.
Key generation
71
Named
Org. Check
70
RQ Org.=
Named Org.
69
B
74
65
66
90
Named MP
Check
68
K2
IBE encryption key K2:
named Medical Organisation +
named Medical Professional (MP)
Insecure
Unauthenticated
Channel 104
Requesting (RQ)
Party
Medical Organisation
Secure
Authenticated
Channel 102
N2
Medical Organisation
T. A.

Figure 8

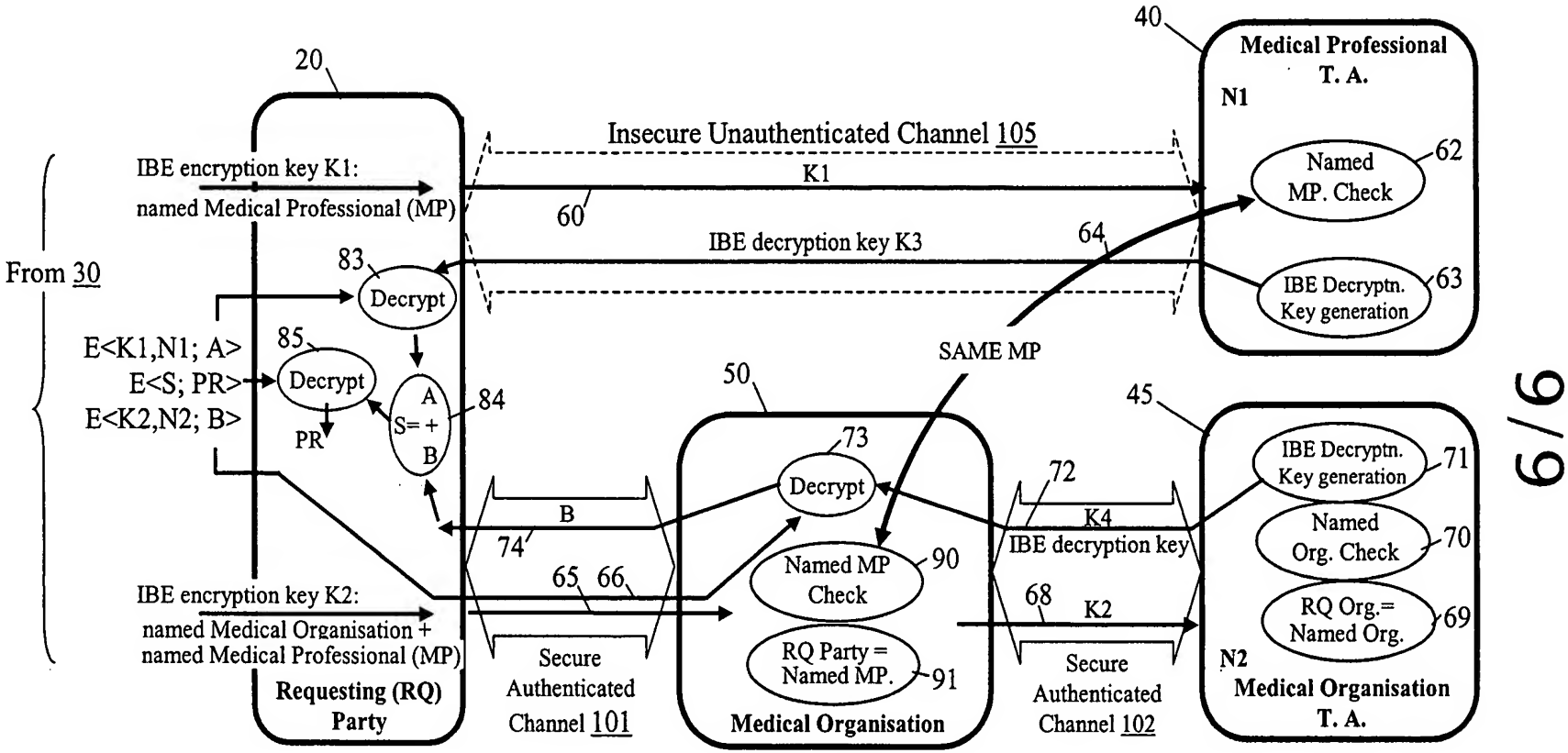

20
40
Medical Professional
T. A.
N1
Insecure Unauthenticated Channel 105
K1
60
IBE encryption key K1:
named Medical Professional (MP)
Named
MP. Check
62
IBE decryption key K3
64
From 30
83
Decrypt
IBE Decryptn.
Key generation
63
SAME MP
E<K1,N1; A>
E<S; PR>
E<K2,N2; B>
85
Decrypt
PR
A
S= +
B
84
50
45
73
Decrypt
72
IBE Decryptn.
Key generation
71
B
74
K4
IBE decryption key
Named
Org. Check
70
Named MP
Check
90
65
66
68
K2
RQ Org.=
Named Org.
69
IBE encryption key K2:
named Medical Organisation +
named Medical Professional (MP)
RQ Party =
Named MP.
91
N2
Secure
Authenticated
Channel 101
Secure
Authenticated
Channel 102
Requesting (RQ)
Party
Medical Organisation
Medical Organisation
T. A.

Figure 9